BLACKBIRD FOR TRAINING

# الأمن السيبراني لأنظمة التحكم الصناعية (ICS)



# الأمن السيبراني لأنظمة التحكم الصناعية (ICS)

## مقدمة

في عالم يعتمد بشكل متزايد على التشغيل الآلي والتحكم الصناعي، أصبحت أنظمة التحكم الصناعية ICS ركيزة أساسية في البنية تحتية للمنشآت الصناعية والطاقة والمرافق الحيوية. ومع توسع الاعتماد على الاتصال بين الشبكات الصناعية وتقنيات المعلومات، ارتفعت المخاطر السيبرانية التي تهدد سلامة واستمرارية العمليات التشغيلية.

تتناول هذه الدورة بعمق مفهوم الأمن السيبراني لأنظمة التحكم الصناعية ICS، وتشرح كيفية حماية الأنظمة التشغيلية من الهجمات السيبرانية، واكتشاف الثغرات الأمنية، وتطبيق استراتيجيات دفاع فعّالة تضمن استمرارية العمل دون تعطيل.

تم تصميم هذا البرنامج لتمكين المهندسين، وخبراء الأمن، ومديري الأنظمة من تطوير مهاراتهم في تحليل المخاطر، تطبيق الأطر الأمنية العالمية، وتصميم بيئات صناعية آمنة ومتينة أمام التهديدات المتطورة.

## أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم البنية الأساسية لأنظمة التحكم الصناعية ومكوناتها الرئيسية.
- التعرف على التهديدات السيبرانية التي تستهدف أنظمة التشغيل الصناعي.
- تطبيق استراتيجيات الدفاع المتعددة الطبقات لحماية الشبكات الصناعية.
- تحليل الحوادث الأمنية والاستجابة الفعالة لها في بيئات ICS.
- استخدام أدوات وتقنيات المراقبة للكشف المبكر عن الهجمات.
- تقييم الامتثال للمعايير الدولية مثل IEC 62443 وNIST.
- تصميم خطط استمرارية الأعمال والتعافي من الكوارث لأنظمة التحكم.



## محاور الدورة

### اليوم الأول: مدخل إلى الأمن السيبراني في الأنظمة الصناعية

- مفهوم الأمن السيبراني في البيئات التشغيلية.
- الفرق بين تكنولوجيا المعلومات IT وأنظمة التشغيل الصناعي OT.
- مكونات أنظمة التحكم الصناعية: SCADA، DCS، وPLC.
- أبرز التهديدات التي تواجه الشبكات الصناعية.
- تحليل أمثلة واقعية لهجمات سيبرانية على منشآت صناعية.

### اليوم الثاني: التهديدات والثغرات في بيئات ICS

- أنواع الهجمات السيبرانية التي تستهدف أنظمة التحكم.
- تحليل الثغرات الأمنية في المكونات المادية والبرمجية.
- أساليب الهندسة الاجتماعية في استهداف العاملين.
- إدارة الوصول والتحكم في الامتيازات داخل الأنظمة الصناعية.
- تقنيات اكتشاف التسلل ومراقبة الشبكات التشغيلية.

### اليوم الثالث: الأطر والمعايير العالمية للأمن الصناعي

- استعراض المعايير الدولية لأمن ICS مثل IEC 62443 وNIST 800-82.
- تطبيق مبدأ الدفاع المتعدد الطبقات Defense-in-Depth.
- إدارة المخاطر الأمنية وفق الأطر المؤسسية.
- بناء سياسات أمنية متكاملة لبيئات التشغيل.
- التوافق مع متطلبات الامتثال التشغيلي والتنظيمي.

### اليوم الرابع: المراقبة، الكشف، والاستجابة للحوادث

- أنظمة المراقبة الأمنية الصناعية SIEM & IDS/IPS.
- تطوير قدرات الاستجابة للحوادث IR.
- تحليل الأدلة الرقمية في الأنظمة الصناعية.
- دور الذكاء الاصطناعي في الكشف المبكر عن الهجمات.
- وضع خطط استجابة عملية للحوادث في بيئات حيوية.



## اليوم الخامس: التصميم الآمن واستمرارية الأعمال

- مبادئ تصميم أنظمة التحكم الصناعية الآمنة.
- استراتيجيات الفصل بين شبكات IT وOT.
- تطوير خطط النسخ الاحتياطي والتعافي من الكوارث.
- التحقق من كفاءة الأنظمة الأمنية عبر الاختبارات الدورية.
- التقييم النهائي ومناقشة المشاريع التطبيقية للمشاركين.

## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- فهم شامل للعلاقة بين الأمن السيبراني والأنظمة التشغيلية الصناعية.
- القدرة على تحليل التهديدات والتعامل معها بطرق عملية.
- اكتساب مهارات تطبيق الأطر الدولية للأمن الصناعي.
- تطوير استراتيجيات دفاع متقدمة ضد الهجمات السيبرانية.
- تحسين جاهزية المؤسسات لمواجهة الأزمات الرقمية.
- تعزيز قدرات الاستجابة السريعة للحوادث التشغيلية.
- بناء خطط مرنة لاستمرارية الأعمال وتقليل المخاطر.
- تطبيق المفاهيم النظرية على حالات واقعية لبيئات صناعية.

## الخاتمة

تُعد أنظمة التحكم الصناعية ICS القلب النابض للمؤسسات الحيوية، لكن تزايد الهجمات الرقمية يجعلها أكثر عرضة للخطر من أي وقت مضى. إن حماية هذه الأنظمة لم تعد خيارًا، بل ضرورة استراتيجية لضمان استمرارية الإنتاج وحماية الأرواح والأصول.

**توفر هذه الدورة فهماً عميقاً لكيفية بناء بيئة صناعية آمنة، قادرة على الصمود أمام التهديدات الحديثة، والتعامل مع الأحداث السيبرانية بسرعة وفعالية. من خلال الدمج بين المعرفة التقنية والخبرة العملية، يصبح المشاركون قادرين على قيادة مبادرات الأمن الصناعي بوعي واحترافية عالية، مما يضمن حماية العمليات واستدامة النجاح في عصر التحول الرقمي.**

